A Novel Approach for the Finding of Clone Node in Wireless Environment for Safe Packet Delivery

Arpita v [1], Dr.Ravindra E [2]

[1]P.G.Student, [2]Professor
Department Of Electronics and Communication Engineering,
GNDEC Bidar, Karnataka (India).

***ABSTRACT*: In this paper, we propose a vitality efficient area mindful clone location convention in thickly conveyed WSNs, which can ensure effective clone assault recognition and keep up acceptable system lifetime. Specifically, we abuse the area data of sensors and haphazardly select witnesses situated in a ring zone to confirm the authenticity of sensors and to report distinguished clone assaults. The ring structure encourages vitality efficient information sending along the way towards the witnesses and the sink. We hypothetically demonstrate that the proposed convention can accomplish 100 percent clone discovery likelihood with trustful witnesses. We additionally broaden the work by concentrating the clone discovery execution with untrustful witnesses and demonstrate that the clone location likelihood still methodologies 98 percent when 10 percent of witnesses are bargained. Also, in most existing clone identification conventions with arbitrary witness choice plan, the required support stockpiling of sensors is normally subject to the hub thickness, while in our proposed convention, the required cradle stockpiling of sensors is autonomous however an element of the bounce length of the system sweep, i.e. Broad reenactments exhibit that our proposed convention can accomplish long system lifetime by adequately conveying the traffic stack over the system.**

***KEYWORDS*: Clone, Energy, System Lifetime**

I. Introduction

Remote sensors have been broadly conveyed for an assortment of uses, running from condition observing to telemedicine and objects following, and so forth [2], [3], [4]. For practical sensor position, sensors are normally not carefully designed gadgets and are sent in spots without observing and insurance, which makes them inclined to various assaults [5], [6], [7], [8]. For instance, a malicious client may trade off a few sensors and procure their private data. At that point, it can copy the sensors and send clones in a remote sensor arrange (WSN) to dispatch an assortment of assaults, which is alluded to as the clone assault. As the copied sensors have a similar data, e.g., code and cryptographic data, caught from honest to goodness sensors, they take an interest in system operations and dispatch assaults. Because of the minimal effort for sensor duplication and sending, clone assaults have turned out to be a standout amongst the most basic security issues in WSNs. In this way, it is fundamental to adequately recognize clone assaults keeping in mind the end goal to guarantee solid operation of WSNs.

II. Related Work

.

1.Z. Zheng et.al(1) proposed an area mindful clone location convention, which ensures fruitful clone assault identification and has minimal negative effect on the system lifetime. In particular, the authors used the area data of sensors and arbitrarily select witness hubs situated in a ring range to confirm the protection of sensors and to distinguish clone assaults. The ring structure encourages vitality productive information sending along the way towards the witnesses and the sink, and the movement load is dispersed over the system, which enhances the system lifetime.

2. T.Shu et.al(5) proposed information conveyance systems that can with high likelihood evade dark openings shaped by these assaults. great multipath steering methodologies are helpless against such assaults, fundamentally because of their deterministic nature. So once the enemy obtains the steering calculation, it can register similar courses known to the source, subsequently, making all data sent over these courses defenseless against its assaults.

3 .R. Lu et.al(7) proposed a system that displayed a powerful plume at social spots (PCS) procedure to accomplish the provable area security. Specifically, they initially presented the social spots where a few vehicles may assemble, e.g., a street crossing point when the movement light turns red or a free parking area close to a shopping center. By taking the secrecy set size as the area security metric, then created two obscurity set diagnostic models to quantitatively research the area protection that is accomplished by the PCS methodology.

4. Z. M. Fadlullah et.al(8) analysed a system that displayed the pernicious as well as irregular occasions, which may bargain the security and protection of savvy network clients, as a Gaussian procedure. In light of this model, a novel early cautioning framework is proposed for expecting pernicious occasions in the SG arrange.

III .System Architecture

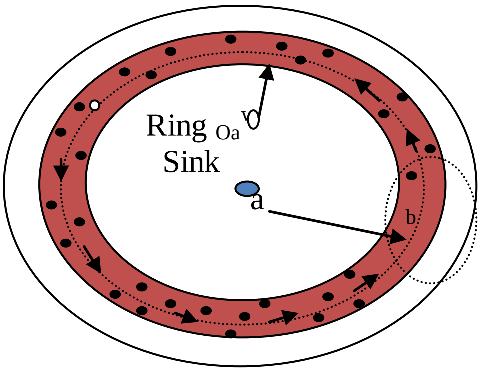

Figure 1: Ring Structure of Witnesses.

Whenever a sensor node establishes a data transmission to others, it has to run the ERCD protocol, i.e,witness selection and legitimacy verification to verify its legitimacy.In witness selection,a ring index is randomly selected by the mapping function as the witness ring of node a. Node a sends its private information to the node located in witness ring,and then the node forwards the information along the witness ring to form a ring structure. The ring index of node a, denoted O_a is compared with its witness ring index O_a^w. Node b stores the private information of node a and forwards the message to any node located in ring O_a^w.

IV. Methodology

We present our circulated clone recognition convention, in particular ERCD convention, which can accomplish a high clone location likelihood with minimal negative effect on system lifetime and restricted necessity of cradle stockpiling limit. The ERCD convention comprises of two phases: witness determination and authenticity verification. In witness determination, an arbitrary mapping capacity is utilized to help each source hub haphazardly select its witnesses. In the authenticity verification, a verification demand is sent from the source hub to its witnesses, which contains the private data of the source hub. On the off chance that witnesses get the verification messages, every one of the messages will be sent to the witness header for authenticity verification, where witness headers are hubs in charge of deciding if the source hub is authenticity or not by looking at the messages gathered from all witnesses. On the off chance that the got messages are not the same as existing record or the messages are lapsed, the witness header will report a clone assault to the sink to trigger a repudiation method. In this paper, we concentrate on outlining a conveyed clone location convention with irregular witness determination by together considering clone discovery likelihood, organize lifetime and information cushion stockpiling. At first, a little arrangement of hubs are bargained by the malevolent clients. Using the clone location convention, we go for augmenting the clone identification likelihood, i.e., the likelihood that cloned hub can be effectively recognized, to guarantee the security of WSNs; in the mean time, the sufficient vitality and cradle stockpiling limit with respect to information gathering and working clone discovery convention ought to be ensured

V. Simulation Results

We present the case that witnesses can be compromised, and thus clone detection may fail due to modification of verification messages by compromised witnesses. For untrustful witnesses, since any witness has permission to read the information of verification messages from the source node, compromised witnesses can read the verification message, and modify (regenerate another modified copy of) the verification message before forwarding it to other witnesses.

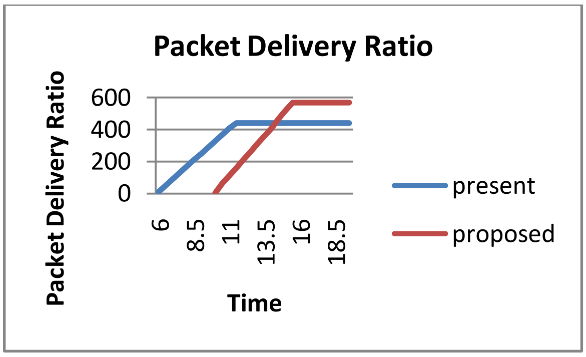

Figure 1: Time Vs Packet Delivery Ratio

Figure 1 shows packet delivery ratio as a function of time. From the graph one can observe that the proposed system is better in packet delivery than the existing system. The red line indicates the proposed system.since the clone is detected while data is transmitted to the destination; packets will not be dropped or stuck into one node only hence packet delivery is higher for proposed one.

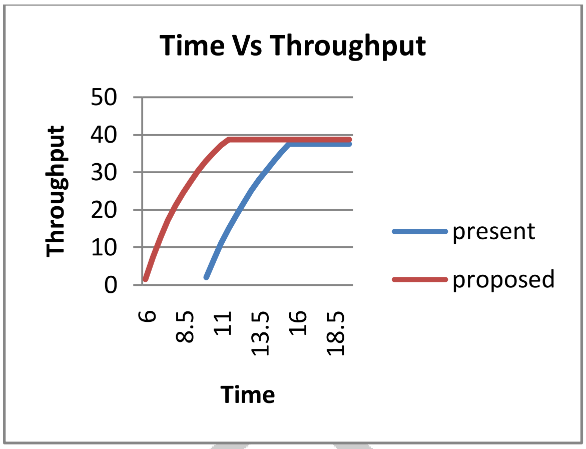

Figure 3: Time Vs Throughput

Figure 3 shows throughput as a function of time.The red line indicates that the proposed system is better in throughputThe clone detection and avoiding those clones while data is transmited makes the throughput better.

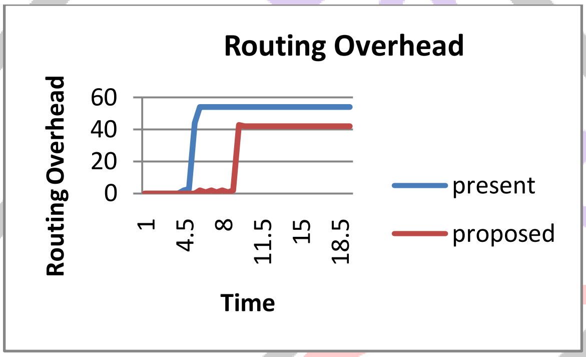

Figure 2: Time Vs Routing Overhead

.

Figure 2 shows routing overhead as a function of time.The graph shows routing overhead is high in proposed system compared to existing system.

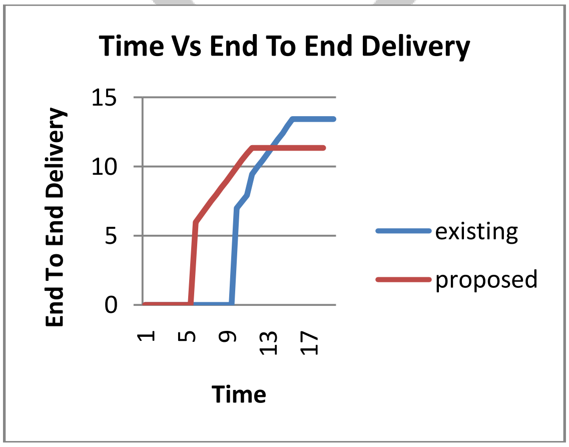

Figure 4: Time Vs End To End Delivery

Figure 4 shows end to end delivery as a function of time.End to end delivery is approximately 15% better for the proposed system.The delay is less because packets will not be dropped and again while transferring the packets the shortest distance and traffic free route is chosen which make the delay to be very less.

VI. Simulation Parameters

Table 1: Simulation Settings and Parameters

Simulation Parameters	Simulation Values
No. of Nodes	33
Area	1100 X 1000
MAC	802.11
Simulation Time	20 Min
Traffic Source	DSR
Rate	50Kb
Propagation	Two Ray Ground
Antenna	Omni Antenna
Initial Energy	200

VII. Conclusion and Future Scope

We have proposed distributed energy-efficient clone detection protocol with random witness selection. Specifically, we have proposed ERCD protocol, which includes the witness selection and legitimacy verification stages. Both of our theoretical analysis and simulation results have demonstrated that our protocol can detect the clone attack with almost probability 1, since the witnesses of each sensor node is distributed in a ring structure which makes it easy be achieved by verification message. In addition, our protocol can achieve better network lifetime and total energy consumption with reasonable storage capacity of data buffer. This is because we take advantage of the location information by distributing the traffic load all over WSNs, such that the energy consumption and memory storage of the sensor nodes around the sink node can be relieved and the network lifetime can be extended.

In our future work, we will consider different mobility patterns under various network scenarios. We can also add the feature of encrypting the packets while transferring to the destination which will make the process even more secured and less vulnerable to the internal attack which is caused by network sensor nodes.

REFERENCES

[1] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, “ERCD: An energy-efficient clone detection protocol in WSNs,” in Proc. IEEE INFOCOM, Apr. 14-19, 2013, pp. 2436–2444.

[2] R.Lu,X.Li,X.Liang, X.Shen, and X.Lin, “GRS: The green, reliability, and security of emerging machine to machine communications,”IEEE Commun.Mag.,vol.49, no.4,pp.28–35,Apr.2011

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, “Wireless sensor networks: A survey,” Comput. Netw., vol. 38, no. 4, pp. 393–422, Mar. 2002.

[4] A. Liu, J. Ren, X. Li, Z. Chen, and X. Shen, “Design principles and improvement of cost function based energy aware routing algorithms for wireless sensor networks,” Comput. Netw., vol. 56, no. 7, pp. 1951–1967, May. 2012.

[5] T. Shu, M. Krunz, and S. Liu, “Secure data collection in wireless sensor networks using randomized dispersive routes,” IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 941–954, Jul. 2010.

[6] P. Papadimitratos, J. Luo, and J. P. Hubaux, “A randomized countermeasure against parasitic adversaries in wireless sensor networks,” IEEE J. Sel. Areas Commun., vol. 28, no. 7, pp. 1036–1045, Sep. 2010.

[7] R. Lu, X. Lin, T. H. Luan, X. Liang, and X. Shen, “Pseudonym changing at social spots: An effective strategy for location privacy in VANETs,” IEEE Trans. Veh. Technol., vol. 61, no. 1, pp. 86–96, Jan. 2012.

[8] Z. M. Fadlullah, M. Fouda, N. Kato, X. Shen, and Y. Nozaki, “An early warning system against malicious activities for smart grid communications,” IEEE Net w., vol. 25, no. 5, pp. 50–55, May. 2011.